IChemE

www.icheme.org/journals
doi: 10.1205/psep.04189

0957–5820/05/$30.00+0.00

Trans IChemE, Part B, September 2005
Process Safety and Environmental Protection, 83(B5): 459–462

CAN CHEMICAL PLANTS BE PROTECTED AGAINST TERRORIST ATTACKS?

C. JOCHUM*

German Major Hazard Commission (Störfallkommission), Robert-Stolz-Str. 54, Baden, Germany

The protection of chemical plants against terrorist attacks became a new challenge after 11 September 2001. In a recent guideline the German Major Hazard Commission describes a "security analysis" to assess the risk of terrorist attacks on chemical plants. Whereas a complete protection never will be possible, a number of well known security and process safety measures are available to reduce the risk, thus making chemical plants to a less attractive target for terrorists. However, conflicts have to be solved between a possible need not to disclose safety information for security reasons and the public's right to know.

Keywords: chemical plants; security; Seveso II directive; terrorist attacks.

Protecting facilities from sabotage and ultimately terrorist attacks has always been one of the duties of the chemical plants operators. This was an important issue in Germany during the time of the Cold War and the threat posed by the "Rote Armee Fraktion" (Red Army Fraction) terrorist group. The disappearance of these threats led to a significant reduction of security measures in many companies. Issues such as transparency and a relaxed way of dealing with employees, customers and visitors came to have more importance than security. In addition, cost-savings could also be made—this is how it appeared at first, anyway.

However, the world has changed since 11 September 2001. The terrorist threat has not only returned but it is more brutal than anyone could ever have previously thought possible. Never before have terrorists sacrificed their own lives so willingly. Never before have they not only simply tolerated the death of large numbers of people but have actually made it their goal. This threat may have been rather increased than decreased as a result of the war in Iraq—as Madrid, 11 March 2004 and London, 7 July 2005 showed in a terrible way. Furthermore, a generally higher level of security may make chemical plants more attractive for terrorists, as attacks on them do not require the infrastructure of terrorist networks and can easily be carried out by fanatic individuals.

To put it in the right perspective: chemical plants do not usually have any particular symbolism and are fortunately therefore not among the preferred targets of terrorist attacks. Targeted attacks on chemical plants are however one of the options of damaging the economy and the infrastructure of the affected country and triggering fear or even panic in the population. Such attacks may seem very unlikely to individual companies but their consequences for employees, neighbours and possibly customers can be dramatic. Recent incidents in chemical plants as in Toulouse 2001 or with chemicals as in North Korea 2004 demonstrate that chemistry may has the potential terrorists are looking for. Moreover, terrorist attacks can jeopardize the existence of even large companies, and insurance cover for such risks is very hard to come by. As a result of this, these issues have to be addressed but, in doing so, the problem must not be overstated, actually providing terrorists with food for thought.

Immediately after 11 September 2001, the Major Hazard Commission at the German Federal Ministry for the Environment ('Störfallkommission') has been assigned to evaluate possible ways to protect chemical and petrochemical plants against terrorist attacks and to prepare a guideline 'Maßnahmen gegen Eingriffe Unbefugter' ('Countermeasures against interference of unauthorized persons'—SFK–GS–38). It issued a preliminary statement within a few months after 11 September 2001. The final guideline is from October 2002 and can be downloaded from www.sfk-taa.de. I will give further details on this below. In the USA, the Centre for Chemical Process Safety (CCPS) issued very detailed 'Guidelines for Analysing and Managing the Security Vulnerabilities of Fixed Installations' in August 2002, to which I will also make some reference. The OECD has performed a workshop 'Public Information Related to Chemical Accidents Resulting from Deliberate Acts' (Rome, 25–27 June 2003). A report is available under www.oecd.org.

First of all, a few words about the **Major Hazard Commission (Störfallkommission, SFK).** In accordance with § 51a of the Federal Immission Control Act, it is made up of representatives of science, environmental groups, trade unions, industry, insurers, expert organizations (TÜV), authorities and the federal institutes/agencies for

**Correspondence to*: Professor Dr C. Jochum, German Major Hazard Commission (Störfallkommission), Robert-Stolz-Str. 54, D 65812 Bad Soden, Germany.
E-mail: chr.jochum@t-online.de

occupational safety and environment. So the Commission's members represent the essential society groups affected by matters of plant safety. The Commission gives advise to the German Federal Government. It's work usually is publicized as reports or guidances, addressing both operators and authorities. These papers are legally not binding, but quite often are adopted by the legislator or the competent authorities.

Now to the guidelines: Both (SFK and CCPS) assume that plants could be considered as preferred targets for terrorists if

- an attack would lead to very serious consequences (the hazard posed by the plant);
- an attack seems relatively easy to carry out (vulnerability);
- the company or the specific plant is particularly 'attractive' due to e.g., some special 'symbolism' (attractiveness).

The SFK Guideline proposes that these aspects should be evaluated using a systematic 'security analysis'. Primary consideration here is given to so called 'upper tier establishments', which are subject to the extended obligations of the Seveso II directive due to the large amounts of hazardous substances and thus 'by definition' represent a particular potential danger. 'Lower tier establishments' or other plants should be considered, too, under certain circumstances. For instance could a major tank of liquefied natural gas in a crowded area cause a severe risk even if its inventory is below the thresholds of the Seveso II directive.

The method of the security analysis consists basically of three steps. In a hazard analysis the question is asked: what can happen by a terrorist attack? The second part of the 'security analysis' is called 'risk analysis' in the SFK Guideline, although this is somewhat contrary to the usual terminology used in the field of process safety. Here it has to be checked how vulnerable and how 'attractive' in the minds of a terrorist the plant could be. The third part are the security measures, preventing attacks and mitigating their consequences.

The Major Hazard Commission tried not to re-invent the wheel, but to make as much use as possible from existing tools. Some points, however, are not 'business as usual' and need specific expertise, may be from an outside consultant. Very important are close links not only to the 'Seveso'-authorities but to the law enforcement and intelligence agencies.

The hazard analysis is used to examine whether an attack on a plant can have serious consequences, particularly due to the high level of risk to a large number of people, dramatic environmental effects or long-term disruption to important supply routes. The question to be answered is therefore what can be assumed as the maximum hazard from a major accident. This is generally equivalent to a scenario which has to be reviewed in the Safety report under the Seveso II directive, which in Germany we call 'Dennoch–Störfall'. This may be translated into 'major accident despite precautions' and is defined as loss of containment, explosion or fire of the largest single quantity of substances.

It must also be determined whether there are facilities in the vicinity of the plant that require particular protection. These might include schools, nurseries, shopping centres, stations or residential areas with high population concentrations. Sensitive establishments will generally be situated outside the site. The transition from traditional chemical plants to industrial parks can, however, mean that 'non-chemical' establishments requiring protecting such as facilities open to the public with large numbers of visitors may also be situated inside the site. It is therefore necessary to evaluate the effects the very serious incidents mentioned above would have for these facilities requiring protection.

All of the information required for the 'hazard analysis' should in principle be available from the safety reports already prepared under the Seveso II guideline. However, it must be ensured that the scenarios for the 'major accident despite precautions' actually take the largest single quantity of substances as their starting point. It is only then that they will cover terrorist attack.

In addition to the risk that can be assumed for a plant, its vulnerability and other aspects of its attractiveness play a decisive role for terrorists. This part of the 'security analysis' is called risk analysis in the SFK Guideline. The following aspects must now be examined:

- the level of threat to the plant and the company;
- the vulnerability of sensitive installations in particular;
- the importance of the plants for the economy of the region;
- any possible symbolism of the company and/or the facilities.

The 'symbolism' of a company is of particular importance to politically motivated terrorists. This symbolism could be due to the fact that it belongs to a strategically/politically exposed group of companies, the type of sales links and activities abroad and the position in society of representatives of the management. These questions show that the task of analysing the terrorist threat can only be delegated to a limited degree within the company. This requires in-depth knowledge of the company, something which can only apply to top management and a handful of other key functions. Close contact with the security authorities and external advisers is also essential for many of the points addressed. An initial screening is, however, possible with the expertise available in most large companies. If the hazard analysis does not produce any significant risks, the risk analysis can simply be omitted.

A company also becomes 'attractive' if it is vulnerable, i.e., easy to attack. The issues of particular importance here are how easily accessible sensitive facilities are with regard to triggering serious disruptions, the structure of the workforce and how effective safety, security and emergency management are. I will demonstrate that it is precisely here that the main starting point of prevention lies.

If it has been shown in these analyses that a plant is both dangerous and at risk, it is necessary to take corresponding steps. Unfortunately, terrorist attacks (as is the case with 'normal' accidents) can never be completely ruled out, particularly not with measures put in place by companies themselves. However, this does not mean that you should do nothing, as is unfortunately sometimes the case. Chemical plants are not top of the list of targets for major terrorists, who ultimately can only be stopped by measures taken by the state. A much more realistic risk is the threat from fanatic individuals acting alone or in loose contact with

others. However, these terrorists can be easily put off by conventional security and preventive measures because, although they may not fear their own death, they do have a real fear that their attack might fail, causing a setback for their cause.

Allow me to make a rather daring comparison to clarify this point. If you install one of the standard burglar alarms in your house, you will hardly ward off a professional thief who knows that you own a valuable Picasso and wants to steal it. However, the opportunist burglar will look for the path of least resistance and thus most likely avoid your house. For a company, this means that the higher the hurdle to entry and to take action, the lower the risk of a terrorist attack, although some risk will always remain.

Prevention basically means impeding unauthorized access into the site as well as to sensitive installations on site and controlling people who are allowed to be inside the site.

Before I now come to the key elements of such safeguarding measures I would like to say that you should not expect something completely new. It is one of the important statements made both by the SFK, the CCPS and in the OECD workshop that conventional security measures, which are in place in a number of chemical companies since years, are effective safeguards against terrorists, too.

The basic measures are

- putting in place external security measures around the plant using fences, and so on, to prevent or at least impede unauthorized entry;
- effective gate control. However, no fence and no gate will stop attacks with high criminal energy. It is therefore of prime importance;
- to monitor these external security measures so that any unauthorized entry can be detected. Here the value of a good fence shows again: it will at least take more time for offenders to come over it, increasing the risk of being detected. In addition to patrols by plant security, modern video technology offers highly effective systems in this field.

The control of people being authorized to stay inside the site has two aspects:

- effective monitoring and supervision of non-employees, such as checking or storing their personal identification cards, arranging for these persons to be picked up from the gate by a company employee or at least confirmation by the person receiving the visitor;
- identifying non-employees by openly wearing visitor and/or company identification cards.

In addition, all methods to detect and alarm process interruptions, monitoring sensitive areas and so on, may make sabotage like acts by internal offenders at least more difficult.

As has already been said, these measures are not new. However, they were less strictly enforced in many companies before 11 September 2001. People did not want to expose themselves to accusations of having a defensive mentality or making the plant a 'high-security wing' as this would also run contrary to the general and highly positive trend towards opening companies up to the outside. Against this background, plant security in many companies had been one of the organizational units which have seen particularly large cutbacks. Whether it be due to a reduction in staff numbers or outsourcing to the cheapest supplier, the quality of and value placed on plant security have fallen sharply in many companies. There must be a change in thinking on the part of top management if long-lasting measures have not already been put in place in the period since 11 September 2001.

For the individual plants within the sites it should also be determined how they can be protected against terrorist attacks. Many of these measures also help to prevent 'normal' accidents and have therefore already been put in place under the headline 'safety'.

The general rule is the higher the level of inherent safety, the less 'vulnerable' the plant. In existing plants, checks should be carried out (again) as to whether the quantities of particularly hazardous substances overall or at least the 'largest single quantity' can be further reduced.

All measures designed to prevent operator error also make things more difficult for potential terrorists. This particularly applies to sabotage by insiders, an issue to which I will return later. Naturally, emergency management with its measures to mitigate the effect of disruptions should also take into consideration the scenarios of a terrorist attack.

In terms of 'normal' accidents, all of these measures are standard in the chemical industry. This should not, however, be taken as an excuse to sit back and relax, but rather as a good starting point to introduce specific measures to defend against terrorism with relatively little outlay and to double effect.

While there are a variety of tried and tested measures for protection against attacks from outside, protection against insider attack is one of the most sensitive points in this context. Unfortunately, the possibility cannot be excluded that contractors or even employees of a company may carry out terrorist attacks themselves or help in their execution. The just mentioned safety measures offer a considerable degree of protection against this threat, too. An effective contractor management should also be mentioned here.

Regarding the own workforce one of the most effective preventive methods is producing a sense of unity, identification with the company and promoting a good working environment in all parts of the company. If this is accompanied by appropriate sensitization of employees to unusual and conspicuous behaviour by colleagues and sensitive and appropriate handling of any conspicuous behaviour, the breeding-ground for potential attack from insiders no longer exists. The German Federal Environment Agency has published a Research Report on this subject (check under www.umweltbundesamt.de).

An important measure in preventing or, to be more precise, impeding terrorist attacks can be keeping sensitive data about a potentially hazardous plant confidential. There is a conflict of objectives here with the right of the public, and especially of neighbours, to get information about potentially hazardous plants—a right which has been increasingly expanded in recent decades. The Seveso II directive has established strict standards in this area.

> Safety reports have to be made available to the public. However, the operator may ask the competent authority not to disclose to the public certain parts of the report, for reasons of industrial, commercial or personal confidentiality, public

> security or national defence. In such cases, on the approval of the competent authority, the operator shall supply to the authority, and make available to the public, an amended report excluding these matters. (Art. 13 para. 4).

The Major Hazard Commission has had detailed and highly controversial discussions on the question of the conditions under which and the extent to which information may be kept confidential. The compromise adopted by a large majority provides that plant-specific data can be kept confidential if—and only if—the analysis of the danger posed by a plant and the level of risk that a plant is exposed to produces a relevant risk of a terrorist attack. This confidentiality should then be limited to information deemed sensitive according to these analyses. A correspondingly adjusted but understandable version of the safety report must be provided for the public.

In addition to the security measures mentioned, a company should check the extent to which the risk of a terrorist attack can be covered by an insurance policy. Such measures are required because, although such attacks are extremely rare, they can lead to damage that jeopardize the existence of the company. The insurance sector, however, hardly feels itself able to cover such risks. A special insurance company, Extremus AG, which offers limited cover for damage resulting from terrorism, was set up for this purpose in Germany. That this insurance cover has yet been bought only by few companies certainly is not only the consequence of a high price. It shows the ongoing problem especially of top management to handle that issue.

The fact that damage resulting from terrorism can jeopardize the existence of a company but cannot be sufficiently covered with an insurance policy makes the preventive and mitigating measures mentioned above all the more important. Management must address these issues. A head-in-the-sand approach to this problem would inevitably lead to accusations of a neglect of duty if anything were to happen. Guidelines such as those from the Major Hazard Commission and the CCPS provide instruments that enable companies to assess the level of risk they face and point out the main protective measures that can be put in place. Specialist consultancy firms are available for more in-depth analysis. Furthermore, it is important that contact is established with the relevant law enforcement and intelligence agencies.

CONCLUSIONS

The answer to the question, if Chemical Plants can be protected against terrorist attacks, fortunately will not be ‘no’. It will be ‘yes, but never completely’. This is quite similar to the situation we are used to in the classical loss prevention area. We can prevent major accidents, but also never completely. In both cases we talk about low probability—high consequences—events, where we have the duty to reduce the risk as far as reasonable possible. I hope I could show that there are a number of instruments available to achieve that. They have to be in relation to the specific risk, of course.

The prevention of and defence against terrorist attacks certainly is a core task of the state. I have, however, tried to underline the fact that it is also within the means of companies to protect themselves from terrorist attacks. Companies which react to this current challenge in a recognizably professional manner will, however, be sure to have better protection against terrorist attacks and thus be less attractive to terrorists.

It is in the interests of management to be ahead of other companies—and the terrorists!—when it comes to this issue. I hope that companies in the chemical industry will regard this as a task which falls under ‘responsible care’ and implement the necessary measures in the very near future, if they have not done it yet completely. It would be highly regrettable if it required a first proven or even only assumed attack to take place and the public pressure triggered as a result for something to be done.

The manuscript was received 15 July 2004 and accepted for publication 10 June 2005.